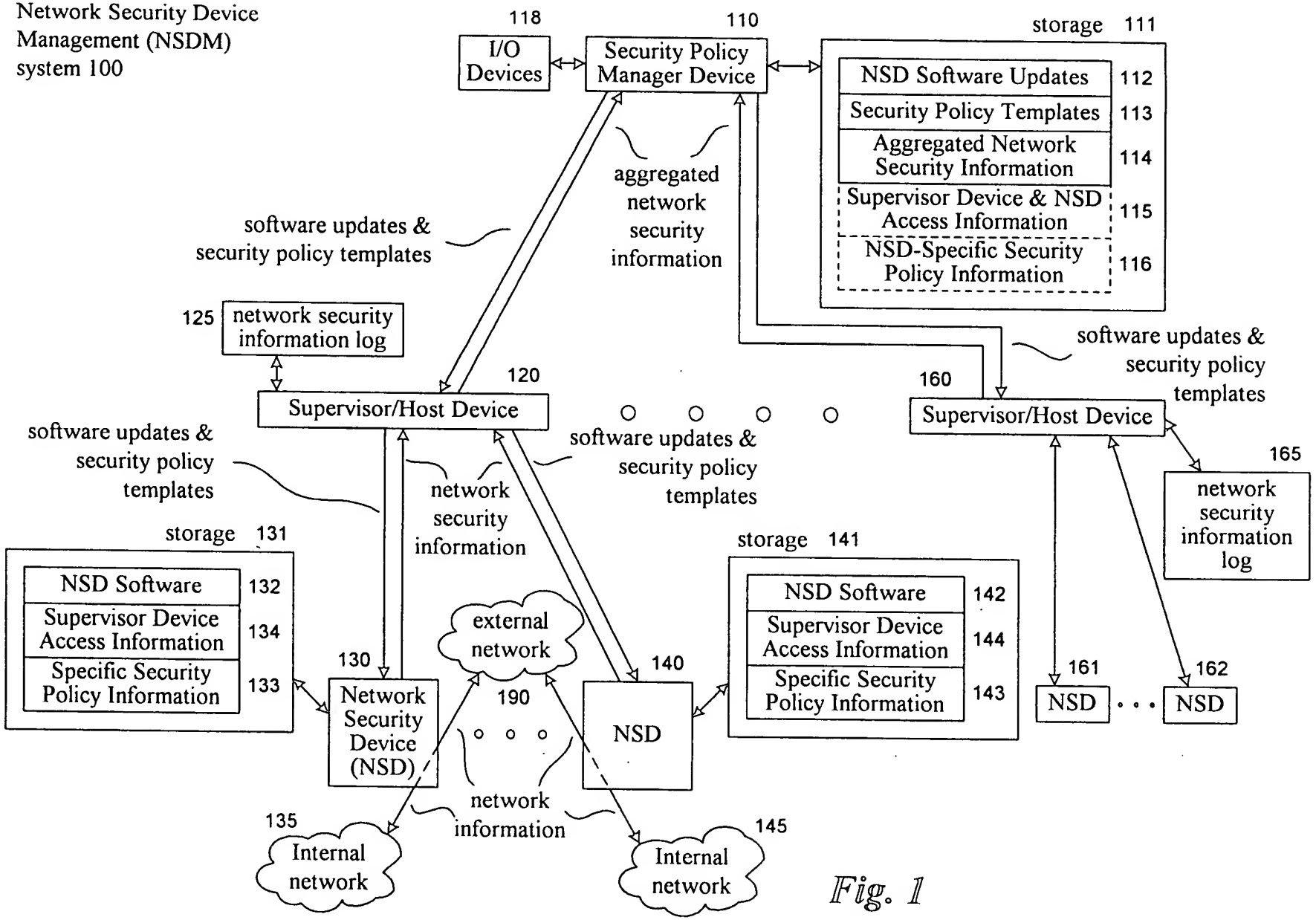
Network Security Device Management (NSDM) system 100
118
I/O Devices
110
Security Policy Manager Device
storage 111
NSD Software Updates 112
Security Policy Templates 113
Aggregated Network Security Information 114
Supervisor Device & NSD Access Information 115
NSD-Specific Security Policy Information 116
aggregated network security information
software updates & security policy templates
125
network security information log
120
Supervisor/Host Device
160
Supervisor/Host Device
software updates & security policy templates
software updates & security policy templates
software updates & security policy templates
165
network security information log
network security information
storage 131
NSD Software 132
Supervisor Device Access Information 134
Specific Security Policy Information 133
storage 141
NSD Software 142
Supervisor Device Access Information 144
Specific Security Policy Information 143
external network
130
Network Security Device (NSD)
190
140
NSD
161
NSD
162
NSD
network information
135
Internal network
145
Internal network

Fig. 1

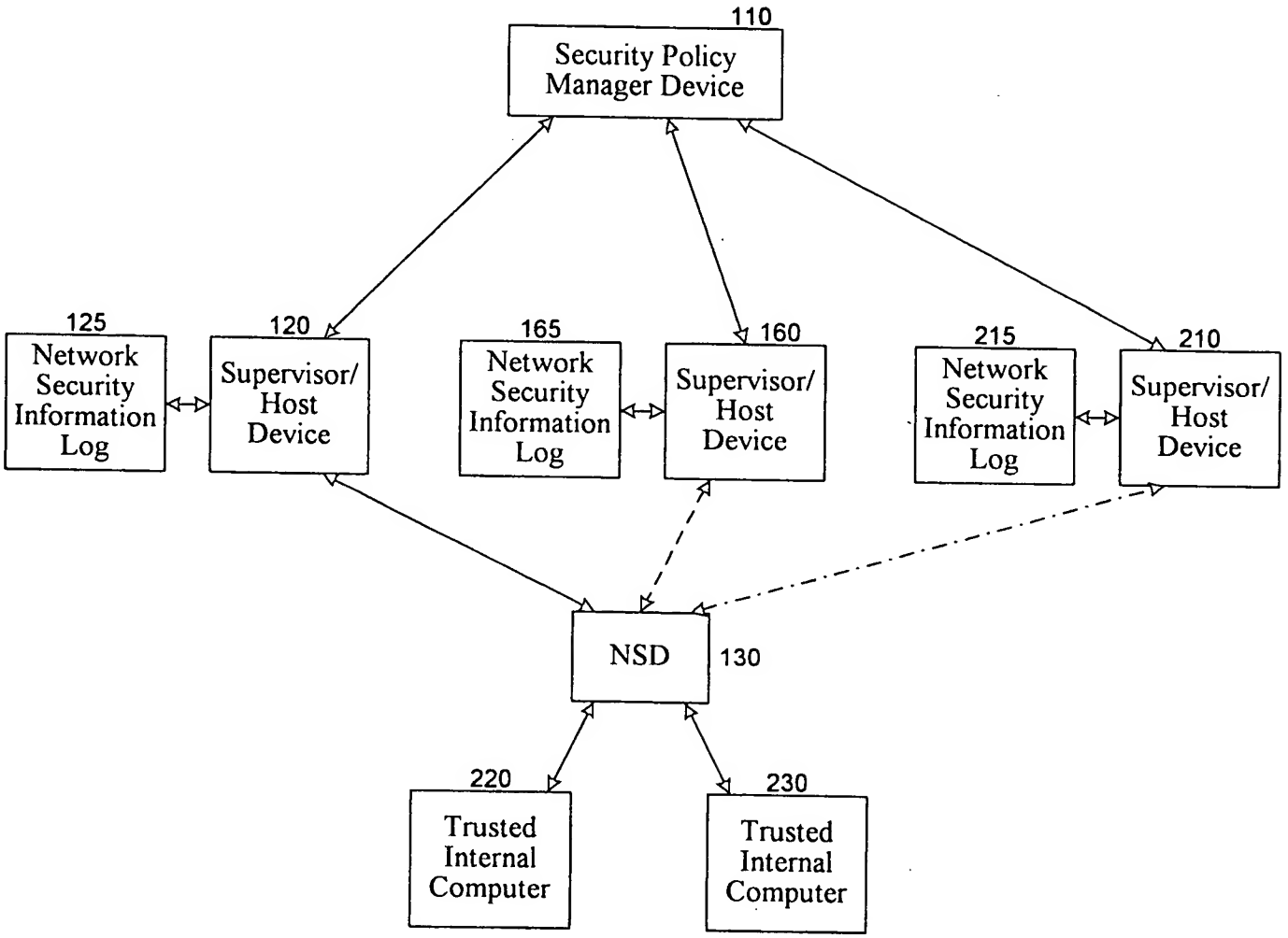
110
Security Policy Manager Device
125
Network Security Information Log
120
Supervisor/ Host Device
165
Network Security Information Log
160
Supervisor/ Host Device
215
Network Security Information Log
210
Supervisor/ Host Device
NSD
130
220
Trusted Internal Computer
230
Trusted Internal Computer

Fig. 2

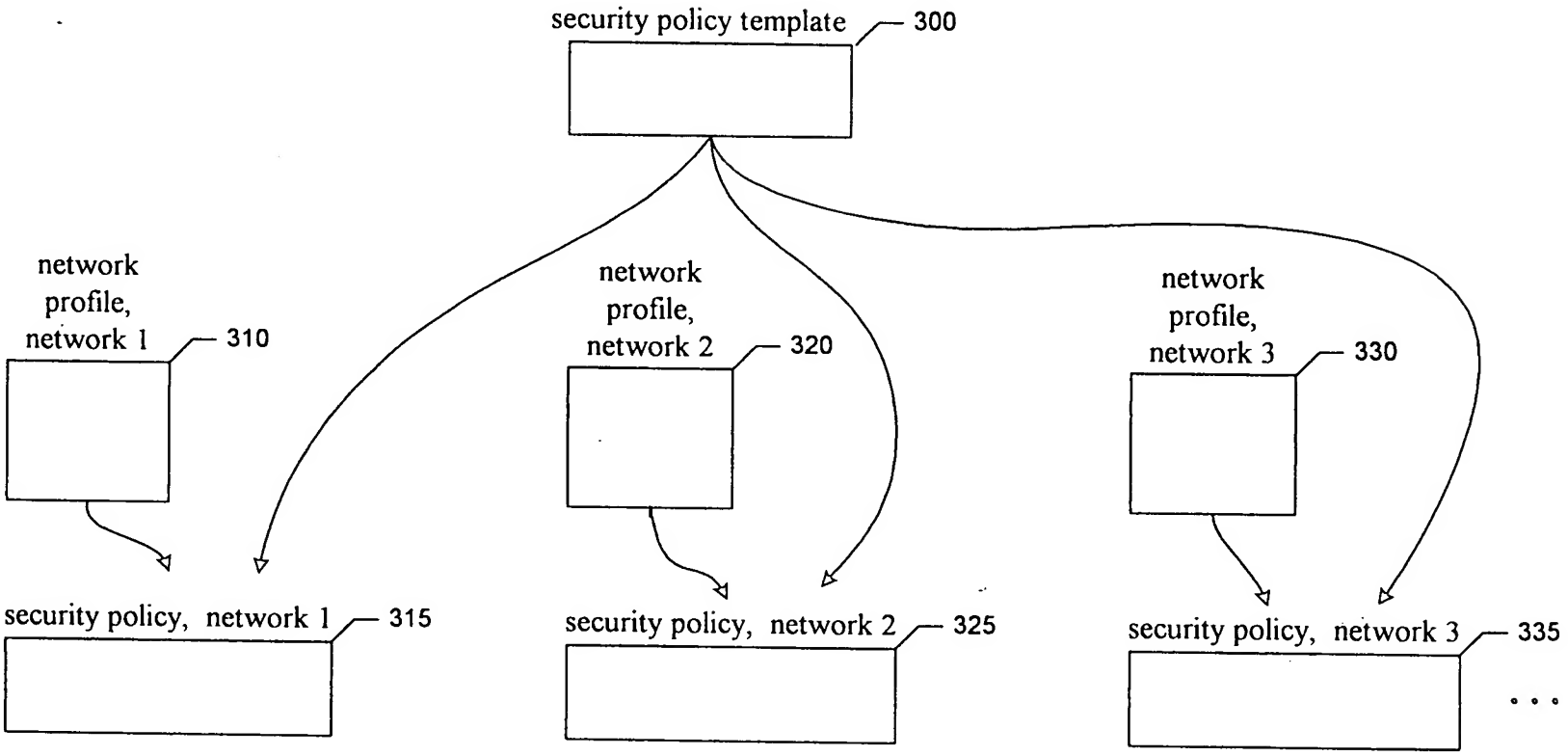
security policy template
300
network
profile,
network 1
310
network
profile,
network 2
320
network
profile,
network 3
330
security policy, network 1
315
security policy, network 2
325
security policy, network 3
335
. . .

Fig. 3A

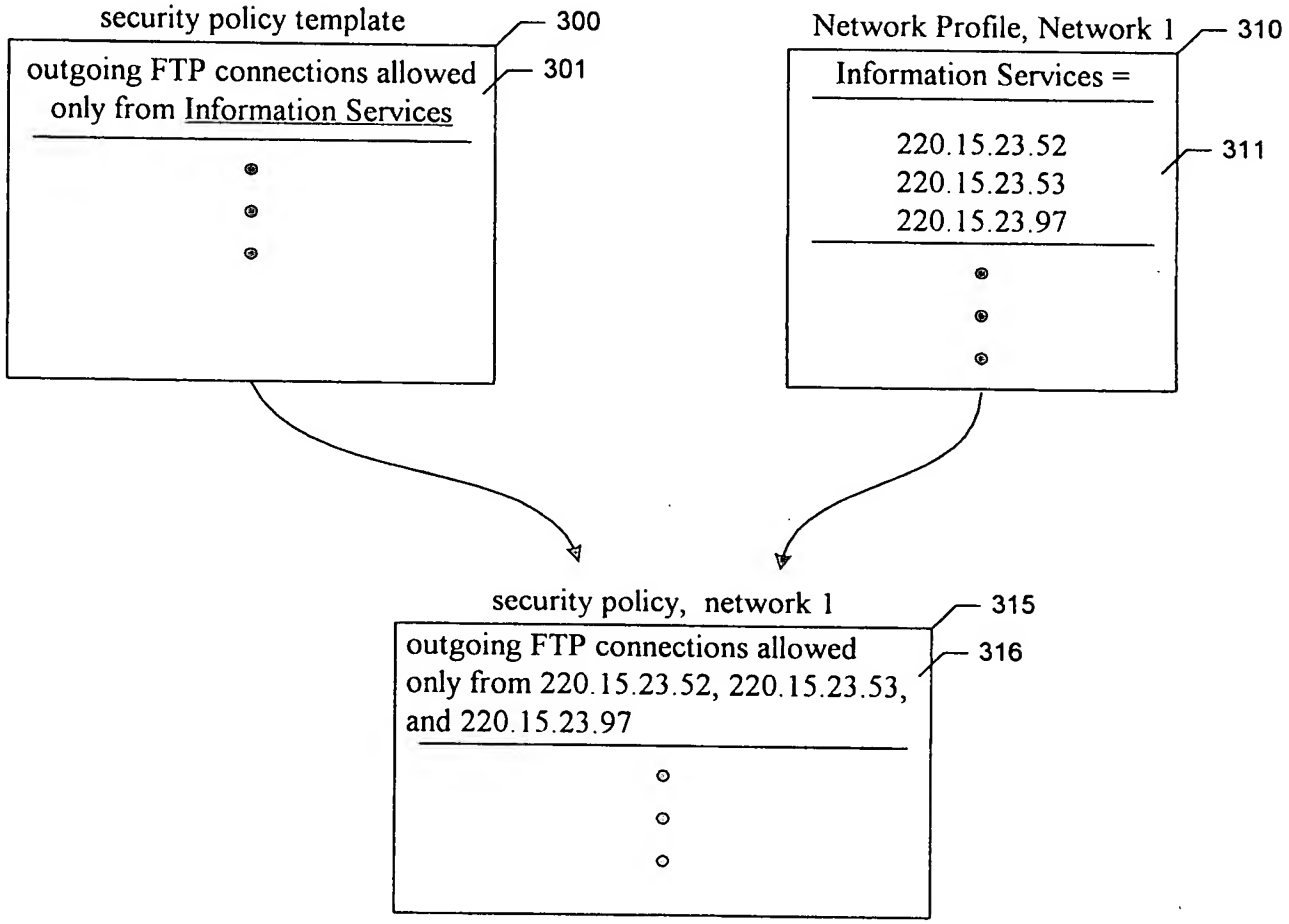
security policy template
300
outgoing FTP connections allowed only from Information Services
301
Network Profile, Network 1
310
Information Services =
220.15.23.52
220.15.23.53
220.15.23.97
311
security policy, network 1
315
outgoing FTP connections allowed only from 220.15.23.52, 220.15.23.53, and 220.15.23.97
316

Fig. 3B

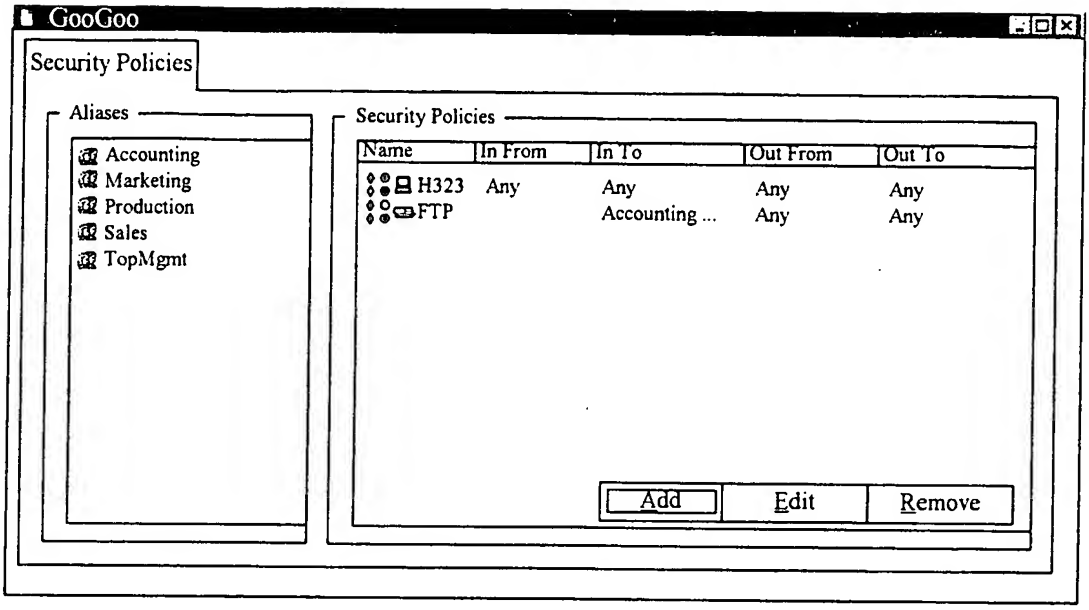
GooGoo
Security Policies
Aliases
Accounting
Marketing
Production
Sales
TopMgmt
Security Policies
Name
In From
In To
Out From
Out To
H323
Any
Any
Any
Any
FTP
Accounting ...
Any
Any
Add
Edit
Remove

FIG. 3C

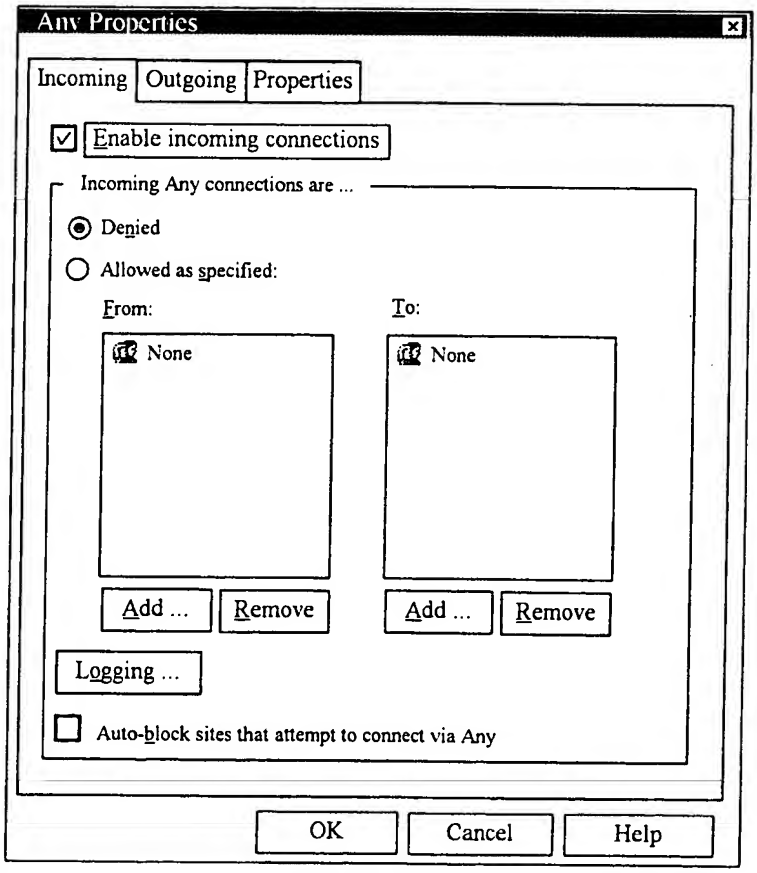
Any Properties
Incoming
Outgoing
Properties
Enable incoming connections
Incoming Any connections are ...
Denied
Allowed as specified:
From:
To:
None
None
Add ...
Remove
Add ...
Remove
Logging ...
Auto-block sites that attempt to connect via Any
OK
Cancel
Help

FIG. 3D

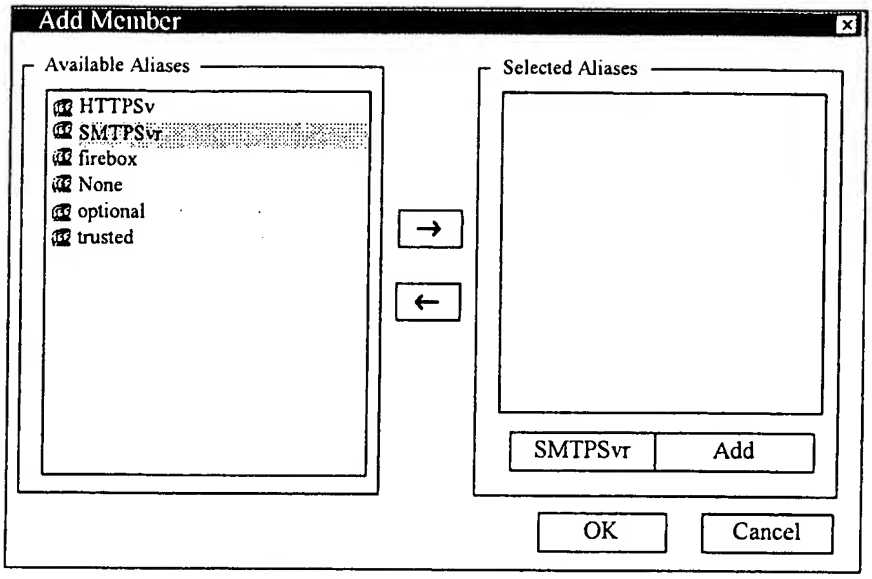
Add Member
Available Aliases
HTTPSv
SMTPSvr
firebox
None
optional
trusted
Selected Aliases
SMTPSvr
Add
OK
Cancel

FIG. 3E

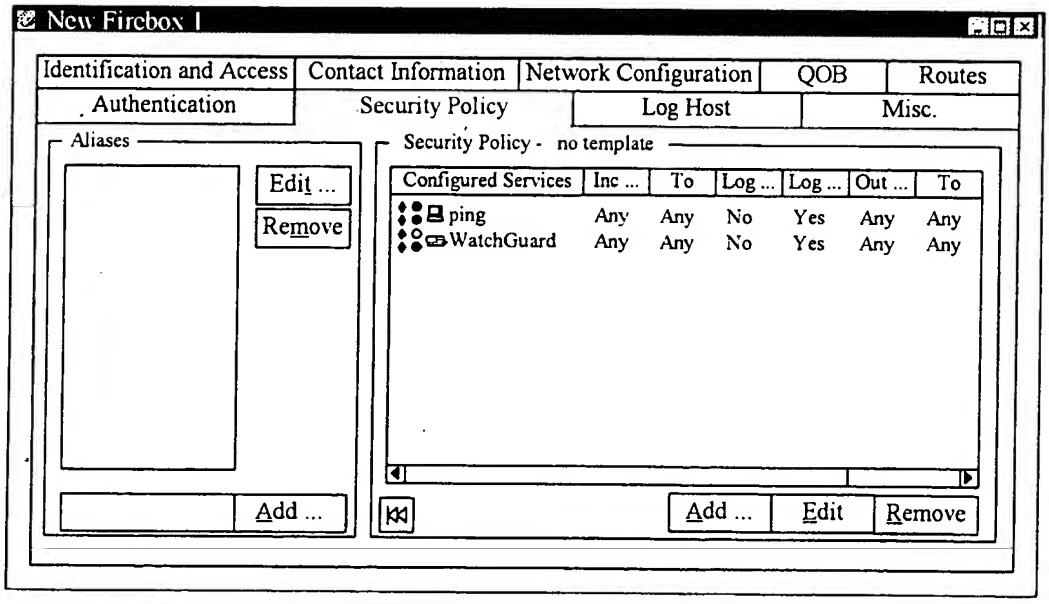
New Firebox I
Identification and Access
Contact Information
Network Configuration
QOB
Routes
Authentication
Security Policy
Log Host
Misc.
Aliases
Edit ...
Remove
Add ...
Security Policy - no template
Configured Services
Inc ...
To
Log ...
Log ...
Out ...
To
ping
Any
Any
No
Yes
Any
Any
WatchGuard
Any
Any
No
Yes
Any
Any
Add ...
Edit
Remove

FIG. 3F

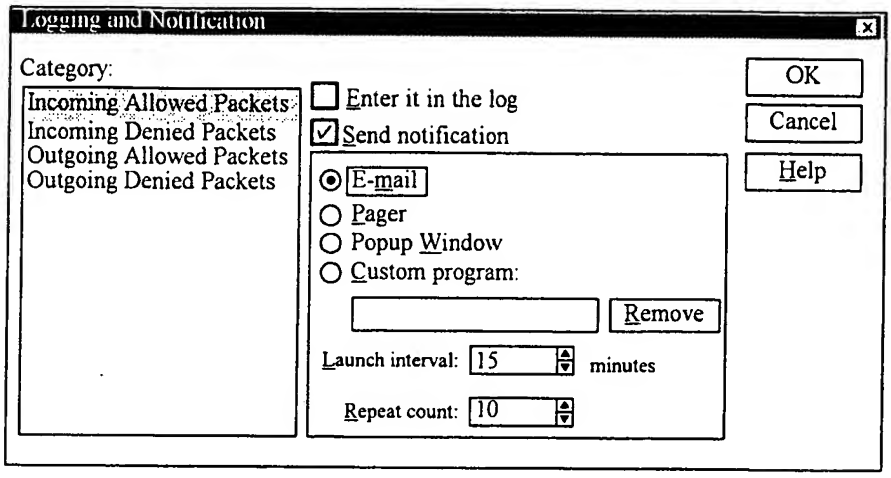
Logging and Notification
Category:
Incoming Allowed Packets
Incoming Denied Packets
Outgoing Allowed Packets
Outgoing Denied Packets
Enter it in the log
Send notification
E-mail
Pager
Popup Window
Custom program:
Remove
Launch interval: 15 minutes
Repeat count: 10
OK
Cancel
Help

FIG. 3G

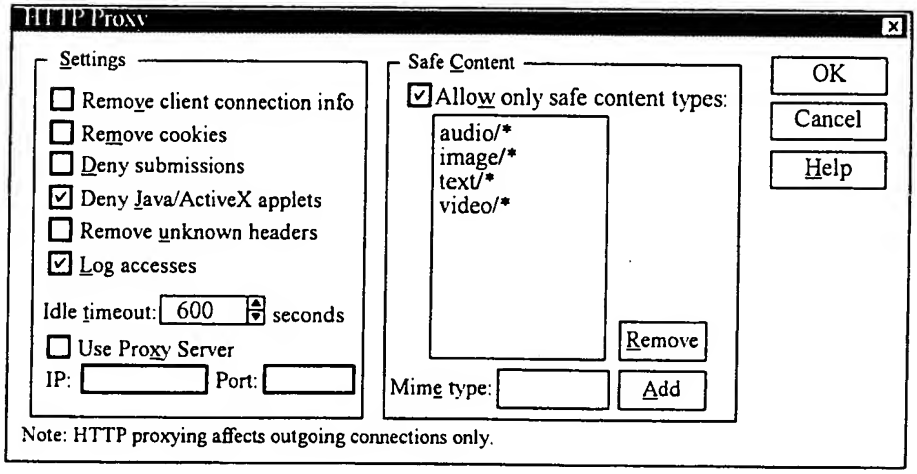
HTTP Proxy
Settings
Remove client connection info
Remove cookies
Deny submissions
Deny Java/ActiveX applets
Remove unknown headers
Log accesses
Idle timeout: 600 seconds
Use Proxy Server
IP:
Port:
Safe Content
Allow only safe content types:
audio/*
image/*
text/*
video/*
Remove
Mime type:
Add
OK
Cancel
Help
Note: HTTP proxying affects outgoing connections only.

FIG. 3H

Jun 15 14:28:15 controld: Firebox closed connection. Hard Close.
Jun 15 14:28:18 controld: WatchGuard controld 3.00.B120 (C) 1996-1998 Watchguard Technologies
Jun 15 14:28:10 10.1.1.1 vpnd [47]: WatchGuard vpnd v3.00.B120 (C) 1996-l 998 WGTI
Jun 15 14:28:10 10.1.1.1 vpnd [47]: No VPN devices configured... exiting.
Jun 15 14:28:10 10.1.1.1 firewalld [48]: Explicitly set external interface was "", auto-detected "eth0"
Jun 15 14:28:10 10.1.1.1 init [1]: WatchGuard Init Copyright (C) 1996-l 998 Watchguard Technologies
Jun 15 14:28:10 10.1.1.1 kernel: Low memory threshhold at 95/90/88 percent.
Jun 15 14:28:10 10.1.1.1 kernel: Console: 16 point font, 400 scans
Jun 15 14:28:10 10.1.1.1 kernel: Console: colour VGA+80x25, 1 virtual console (max 63)
Jun 15 14:28:10 10.1.1.1 kernel: pcibios_init : BIOS32 Service Directory structure at 0x000fadc0
Jun 15 14:28:10 10.1.1.1 kernel: pcibios_init : BIOS32 Service Directory entry at 0xfb230
Jun 15 14:28:10 10.1.1.1 kernel: pcibios_init : PCI BIOS revision 2.10 entry at 0xfb260
Jun 15 14:28:10 10.1.1.1 kernel: Probing PC1 hardware.
Jun 15 14:28:10 10.1.1.1 kernel: Warning : Unknown PC1 device (1023: 9660). Please read include/linux/pci.h
Jun 15 14:28:10 10.1.1.1 kernel: Calibrating delay loop.. ok -35.94 BogoMIPS
Jun 15 14:28:10 10.1.1.1 kernel: Memory: 15000k/l6384k available (540k kernel code, 384k reserved, 460k data)
Jun 15 14:28:10 10.1.1.1 kernel: Swansea University Computer Society NET3.035 for Linux 2.0
Jun 15 14:28:10 10.1.1.1 kernel: NET3: Unix domain sockets 0.13 for Linux NET3.035.
Jun 15 14:28:10 10.1.1.1 kernel: Swansea University Computer Society TCP/IP for NET3.034
Jun 15 14:28:10 10.1.1.1 kernel: IP Protocols: ICMP, GRE, UDP, TCP
Jun 15 14:28:10 10.1.1.1 kernel: Checking 3861387 coupling... Ok, fpu using exception 16 error
Jun 15 14:28:10 10.1.1.1 kernel: Checking 'hlt' instruction... Ok.
Jun 15 14:28:10 10.1 .l. l kernel: Intel Pentium with F0 0F bug - workaround enabled.
Jun 15 14:28:10 10.1.1.1 kernel: alias mapping IDT readonly ... ... done
Jun 15 14:28:10 10.1.1.1 kernel: Linux version 2.0.33 (bryan@terror) (gcc version 2.7.2.1) #1 Wed Apr 22 12:00:23 PDT 1998
Jun 15 14:28:10 10.1.1.1 kernel: Starting kswapd v 1.2
Jun 15 14:28:10 10.1.1.1 kernel: Serial driver version 4.13 with no serial options enabled
Jun 15 14:28:10 10.1.1.1 kernel: tty00 at 0x03f8 (irq=4) is a 16550A
Jun 15 14:28:10 10.1.1.1 kernel: tty01 at 0x02f8 (irq=3) is a 16550A
Jun 15 14:28:10 10.1.1.1 kernel: Real Time Clock Driver v1.07
Jun 15 14:28:10 10.1.1.1 kernel: Ramdisk driver initialized : 16 ramdisks of 4096K size
Jun 15 14:28:10 10.1.1.1 kernel: Floppy drive(s) : fd0 is 1.44M

FIG. 4A

Jun 15 14:28:10 10.1.1.1 kernel: FDC 0 is an 8272A
Jun 15 14:28:10 10.1.1.1 kernel: eth0: 3c509 at 0x300 tag 1, 10baseT port, address 00 60 97 97 a3 06, IRQ 9.
Jun 15 14:28:10 10.1.1.1 kernel: 3c509.c:1.12 6/4/97 becker@cesdis.gsfc.nasa.gov
Jun 15 14:28:10 10.1.1.1 kernel: eth1: 3c509 at 0x320 tag 2, 10baseT port, address 00 60 97 a9 c1 42, IRQ 10.
Jun 15 14:28:10 10.1.1.1 kernel: 3c509.c:1.12 6/4/97 becker@cesdis.gsfc.nasa.gov
Jun 15 14:28:10 10.1.1.1 kernel: eth2: 3c509 at 0x340 tag 3, 10baseT port, address 00 60 97 ad c5 2b, IRQ 11.
Jun 15 14:28:10 10.1.1.1 kernel: 3c509.c:1.12 6/4/97 becker@cesdis.gsfc.nasa.gov
Jun 15 14:28:10 10.1.1.1 kernel: VFS: Disk change detected on device 02:00
Jun 15 14:28:10 10.1.1.1 kernel: RAMDISK: Compressed image found at block 440
Jun 15 14:28:10 10.1.1.1 kernel: VFS: Mounted root (minix filesystem) readonly.
Jun 15 14:28:10 10.1.1.1 kernel: WatchGuard Driver v3.00.B120 (C) 1995-1998 WGTI
Jun 15 14:28:10 10.1.1.1 firewalld [48]: new outside interface is eth0
Jun 15 14:28:10 10.1.1.1 firewalld [48]: Starting child /bin/server
Jun 15 14:28:11 10.1.1.1 firewalld [48]: Starting child /opt/bin/tunneld
Jun 15 14:28:11 10.1.1.1 h323 [52]: WatchGuard h323 v3.00.Bl20 (C) 1998 WGTI
Jun 15 14:28:11 10.1.1.1 sw-proxy [53]: streamworks-proxy launched
Jun 15 14:28:11 10.1.1.1 firewalld [48]: Starting child /opt/bin/webblocker
Jun 15 14:28:11 10.1.1.1 kernel: WG: reset
Jun 15 14:28:11 10.1.1.1 firewalld [48]: Couldn't find property options.portfwd.hosts, returning ""
Jun 15 14:28:11 10.1.1.1 dce_rpc [54]: WatchGuard dce_rpc v3.00.B120 (C) 1998 WGTI
Jun 15 14:28:12 10.1.1.1 tunneld [56]: WatchGuard PPTP-tunneld v3.00.Bl20 (C) 1997-1998 WGTI
Jun 15 14:28:12 10.1.1.1 kernel: PPTP: version 1.0.0 (For export)
Jun 15 14:28:12 10.1.1.1 kernel: MPPC: will not compress outgoing packets
Jun 15 14:28:12 10.1.1.1 tunneld [56]: added 1 pptp interfaces
Jun 15 14:28:12 10.1.1.1 tunneld [56]: software compression will not be negotiated
Jun 15 14:28:12 10.1.1.1 nbrecast [60]: WatchGuard NBRecast v3.00.Bl20 (C) 1998 WGTI
Jun 15 14:28:12 10.1.1.1 tunneld [61]: messenger_init: using syslog as printer (with LOG_WARNING level)
Jun 15 14:28:12 10.1.1.1 tunneld [61]: messenger_init: will read from /tmp/message.61 file
Jun 15 14:28:12 10.1.1.1 firewalld [48]: WatchGuard Daemon, v3.00.Bl20 (C) 1996-1998 WGTI
Jun 15 14:28:12 10.1.1.1 firewalld [48]: Couldn't connect daytime socket (Connection refused)
Jun 15 14:28:12 10.1.1.1 firewalld [48]: Childmax is 490
Jun 15 14:28:12 10.1.1.1 firewalld [48]: Pid 57, exit status 0

FIG. 4B

Jun 15 14:28:12 10.1.1.1 firewalld [48]: Pid 56, exit status 0
Jun 15 14:28:12 10.1.1.1 http-proxy [58]: WatchGuard HTTP proxy v3.00.B120 (C) 1996-1998 WGTI
Jun 15 14:28:17 10.1.1.1 authentication [55]: WatchGuard authentication v3.00.B120 (C) 1998 WGTI
Jun 15 14:28:25 10.1.1.1 fwcheck [51]: fwcheck (C) 1998 WGTI
Jun 15 14:28:53 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:30:08 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:31:29 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:32:52 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:33:08 10.1.1.1 http-proxy [78]: [10.1.1.15:1094 204.202.129.247:80/java/ScorePost.zip] Response from 204.202.129.247:80/java/scorepost.zip denied: Unsafe content type "application/zip"
Jun 15 14:33:08 10.1.1.1 http-proxy [79]: [10.1.1.15:1095 204.202.129.247:80/java/starwave/sportszone/scorepost/ScorePost.class] Response from 204.202.129.247:80/java/starwave/sportszone/scorepost/scorepost.class denied: Unsafe content type
Jun 15 14:33:08 10.1.1.1 http-proxy [80]: [10.1.1.15:1096 204.202.129.230:80/javanew/lw_ticker/LWScroller.class] Response from 204.202.129.230:80/javanew/lw_ticker/lwscroller.class denied: Unsafe applet
Jun 15 14:34:21 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:35:42 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:37:01 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:38:22 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:39:51 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:41:17 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:42:30 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:43:45 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:45:10 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:46:38 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:48:00 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:49:28 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:50:42 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:51:58 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:53:11 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:54:36 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:55:53 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 14:57:23 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)

FIG. 4C

Jun 15 14:57:57 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 63 208.152.24.33 208.152.24.23 3946 113 syn (default)
Jun 15 14:58:35 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:00:04 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:01:29 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:02:49 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:04:14 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:05:39 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:05:54 10.1.1.1 http-proxy [205]: [10.1.1.15:1144
208.134.241.152:80/js.ng/Params.richmedia=yes&uniqueID=homepage.main.0&GroupID=400&PagePos=1] Response from
208.134.241.152:80/js.ng/params.richmedia=yes&uniqueid=homepage.main.0&grou
Jun 15 15:06:10 10.1.1.1 http-proxy [209]: [10.1.1.15:1148
208.134.241.152:80/js.ng/Params.richedia=yes&uniquelD=homepage.main.0&GroupID=400&PagePos=1] Response from
208.134.241.152:80/js.ng/params.richmedia=yes&uniqueid=homepage.main.0&grou
Jun 15 15:06:10 10.1.1.1 http-proxy [210]: [10.1.1.15:1149 208.134.241.155:80/homepage/pics/forecasts_conditions_450.gif] Can't
send data to client (Broken pipe)
Jun 15 15:06:10 10.1.1.1 http-proxy [208]: [10.1.1.15:1147 208.134.241.155:80/breaking_weather/live_story/pics/hmpg_image.jpg]
Can't send data to client (Broken pipe)
Jun 15 15:06:10 10.1.1.1 http-proxy [211]: [10.1.1.15:1150 208.134.241.155:80] relaying connection-reset (on read) from client
Jun 15 15:07:06 10.1.1.1 http-proxy [262]: [10.1.1.15:1207 204.133.127.77:80/java/Ticker.class] Response from
204.133.127.77:80/java/ticker.class denied: Unsafe applet
Jun 15 15:07:08 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:08:35 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:09:50 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:09:59 10.1.1.1 http-proxy [309]:[l0.1.1.17:1074 206.35.113.28:80/F/OCVscroll.class] Response from
206.35.113.28:80/f/ocvscroll.class denied: Unsafe content type "application/octet-stream"
Jun 15 15:10:00 10.1.1.1 http-proxy [310]: [10.1.1.17:1075 206.35.113.28:80/F/resbar.gif] Can't send data to client (Broken pipe)
Jun 15 15:10:00 10.1.1.1 http-proxy [311]: [10.1.1.17:1076 206.35.113.28:80/F/331.gif] Can't send data to client (Broken pipe)
Jun 15 15:10:00 10.1.1.1 http-proxy [312]: [10.1.1.17:1077 206.35.113.28:80/F/copyrigh.gif] Can't send data to client (Broken pipe)
Jun 15 15:10:00 10.1.1.1 http-proxy [313]: [10.1.1.17:1078 206.35.113.28:80] relaying connection-reset (on read) from client
Jun 15 15:11:03 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:12:19 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:13:32 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)

FIG. 4D

Jun 15 15:13:53 10.1.1.1 http-proxy [336]: [10.1.1.21:1034 206.69.91.l00:80/neonews/Scroll.class] Response from 206.69.91.100:80/neonews/scroll.class denied: Unsafe applet
Jun 15 15:14:21 10.1.1.1 http-proxy [349]: [10.1.1.21:1048 141.142.3.70:80/java/mamagator.class] Response from 141.142.3.70:80/java/mamagator.class denied: Unsafe content type "application/octet-stream"
Jun 15 15:14:54 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:16:12 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:17:29 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:18:53 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:19:58 10.1.1.1 http-proxy [382]: [10.1.1.19:1027 207.25.71.22:80/virtual/1998/code/cnn.js] Response from 207.25.71.22:80/virtual/1998/code/cnn.js denied: Unsafe content type "application/x-javascript"
Jun 15 15:20:11 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:20:28 10.1.1.1 http-proxy [393]: [10.1.1.19:1041 204.152.178.145:80/phrack52.tar.gz] Response from 204.152.178.145:80/phrack52.tar.gz denied: Unsafe content type "application/x-tar"
Jun 15 15:21:37 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:22:52 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:24:12 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:25:36 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:27:03 10.1.1.1 firewalld [48]: deny in eth0 4o 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:28:21 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:29:37 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:30:51 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:31:03 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 63 208.152.24.33 208.152.24.23 4124 113 syn (default)
Jun 15 15:32:20 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:33:33 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:34:48 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:36:02 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2208.152; 24.30 255.255.255.255 (default)
Jun 15 15:37:21 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:37:39 10.1.1.1 firewalld [48]: deny in eth0 56 icmp 20 255 208.152.24.30 208.152.24.23 5 1 (default)
Jun 15 15:38:44 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:40:00 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:41:22 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:41:55 10.1.1.1 http-proxy [585]: [10.1.1.20:1029 192.215.74.11:80] relaying connection-reset (on read) from client

FIG. 4E

Jun 15 15:42:45 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:44:10 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:45:33 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:46:43 10.1.1.1 http-proxy[610]: [10.1.1.25:1030 209.67.29.11:80/java/NewsTicker/NewsTicker1.class] Response from 209.67.29.11:80/java/newsticker/newsticker1.class denied: Unsafe applet
Jun 15 15:46:48 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:46:54 10.1.1.1 http-proxy [617]: [10.1.1.25:1037 209.67.29.11:80] relaying connection-reset (on read) from client
Jun 15 15:46:55 10.1.1.1 http-proxy [627]: [10.1.1.25:1047 209.67.29.11:80] relaying connection-reset (on read) from client
Jun 15 15:48:09 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:49:34 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:51:03 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:52:04 10.1.1.1 http-proxy [670]: [10.1.1.30:1061 206.99.97.11:80] connection timed out: exiting
Jun 15 15:52:18 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:53:31 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 15:54:36 10.1.1.1 http-proxy [704]: [10.1.1.30:1096 206.99.97.11:80] connection timed out: exiting
Jun 15 15:56:19 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255
Jun 15 15:57:46 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255
Jun 15 15:59:09 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255
Jun 15 16:00:24 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255
Jun 15 16:01:42 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255
Jun 15 16:03:01 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255
Jun 15 16:04:22 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255
Jun 15 16:04:25 10.1.1.1 http-proxy [763]: [10.1.1.24:1047 168.100.205.221:80] relaying connection-reset (on read) from client
Jun 15 16:05:39 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:07:08 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:08:31 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:09:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1024 4102 syn (default)
Jun 15 16:09:25 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1024 4102 syn (default)
Jun 15 16:09:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1030 4102 syn (default)
Jun 15 16:09:55 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:10:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1031 4102 syn (default)

FIG. 4F

Jun 15 16:10:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1037 4102 syn (default)
Jun 15 16:11:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1090 4102 syn (default)
Jun 15 16:11:25 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:11:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1095 4102 syn (default)
Jun 15 16:12:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1096 4102 syn (default)
Jun 15 16:12:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1152 4102 syn (default)
Jun 15 16:12:55 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:13:08 10.1.1.1 http-proxy [825]: [10.1.1.23:1042 204.202.129.247:80/java/ScorePost.zip] Response from 204.202.129.247:80/java/scorepost.zip denied: Unsafe content type "application/zip"
Jun 15 16:13:09 10.1.1.1 http-proxy [826]: [10.1.1.23:1043 204.202.129.247:80/java/starwave/sportszone/scorepost/ScorePost.class] Response from 204.202.129.247:80/java/starwave/sportszone/scorepost/scorepost.class denied: Unsafe content type
Jun 15 16:13:09 10.1.1.1 http-proxy [827]: [10.1.1.23:1044 204.202.129.230:80/javanew/lw_ticker/LWScroller.class] Response from 204.202.l29.230:80/javanew/lw_ticker/lwscroller.class denied: Unsafe applet
Jun 15 16:13:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1216 4102 syn (default)
Jun 15 16:13:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1283 4102 syn (default)
Jun 15 16:14:20 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:14:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1284 4102 syn (default)
Jun 15 16:14:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1285 4102 syn (default)
Jun 15 16:15:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1286 4102 syn (default)
Jun 15 16:15:37 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:15:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1287 4102 syn (default)
Jun 15 16:16:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1288 4102 syn (default)
Jun 15 16:16:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1294 4102 syn (default)
Jun 15 16:17:02 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:17:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1297 4102 syn (default)
Jun 15 16:17:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1298 4102 syn (default)
Jun 15 16:18:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1361 4102 syn (default)
Jun 15 16:18:31 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:18:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1362 4102 syn (default)
Jun 15 16:19:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1424 4102 syn (default)
Jun 15 16:19:49 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:19:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1488 4102 syn (default)

FIG. 4G

Jun 15 16:20:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1559 4102 syn (default)
Jun 15 16:20:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1563 4102 syn (default)
Jun 15 16:21:04 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:21:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1564 4102 syn (default)
Jun 15 16:21:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1565 4102 syn (default)
Jun 15 16:22:22 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1567 4102 syn (default)
Jun 15 16:22:29 10.1.1.1 firewalld [48]: deny in eth0 46 9 20 2 208.152.24.30 255.255.255.255 (default)
Jun 15 16:22:52 10.1.1.1 firewalld [48]: deny in eth0 44 tcp 20 53 198.245.206.12 208.152.24.23 1569 4102 syn (default)
Jun 15 16:23:53 controld: Error: Connection reset by peer. Receive: error #l0054
Jun 15 16:23:57 controld: WatchGuard controld 3.00.B120 (C) 1996-l998 Watchguard Technologies
Jun 11 02:43:58 198.245.206.12 firewalld [49]: deny in ethl 242 udp 20 32 198.245.206.208 198.245.206.255 138 138 (SMB)
Jun 15 16:24:13 controld: WatchGuard controld 3.00.B120 (C) 1996-l998 Watchguard Technologies

FIG. 4H

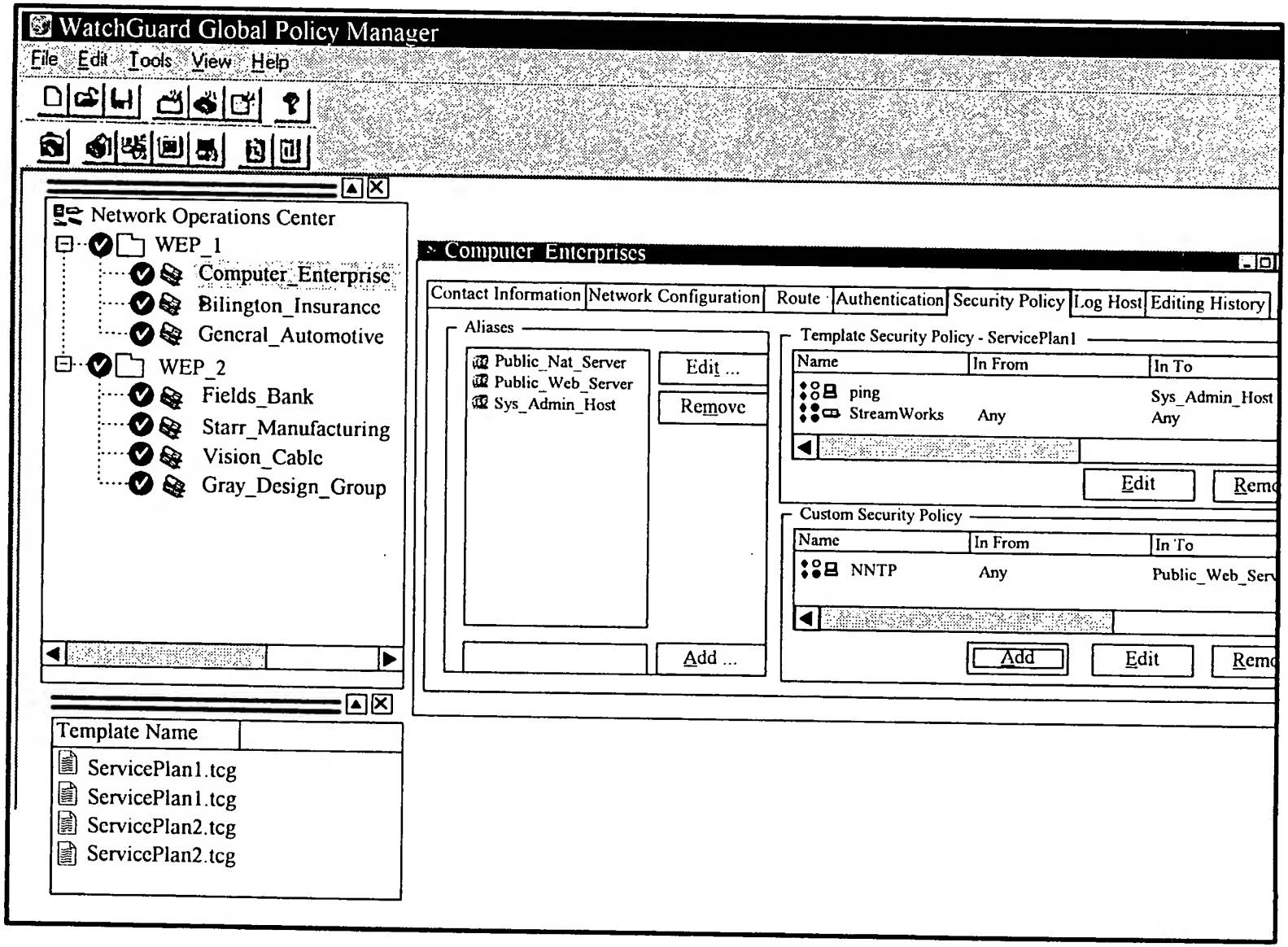
WatchGuard Global Policy Manager
File Edit Tools View Help
Network Operations Center
WEP_1
Computer_Enterprise
Bilington_Insurance
General_Automotive
WEP_2
Fields_Bank
Starr_Manufacturing
Vision_Cable
Gray_Design_Group
Computer Enterprises
Contact Information
Network Configuration
Route
Authentication
Security Policy
Log Host
Editing History
Aliases
Public_Nat_Server
Public_Web_Server
Sys_Admin_Host
Edit ...
Remove
Add ...
Template Security Policy - ServicePlan1
Name
In From
In To
ping
Sys_Admin_Host
StreamWorks
Any
Any
Edit
Custom Security Policy
NNTP
Any
Add
Edit
Template Name
ServicePlan1.tcg
ServicePlan1.tcg
ServicePlan2.tcg
ServicePlan2.tcg

FIG. 5A

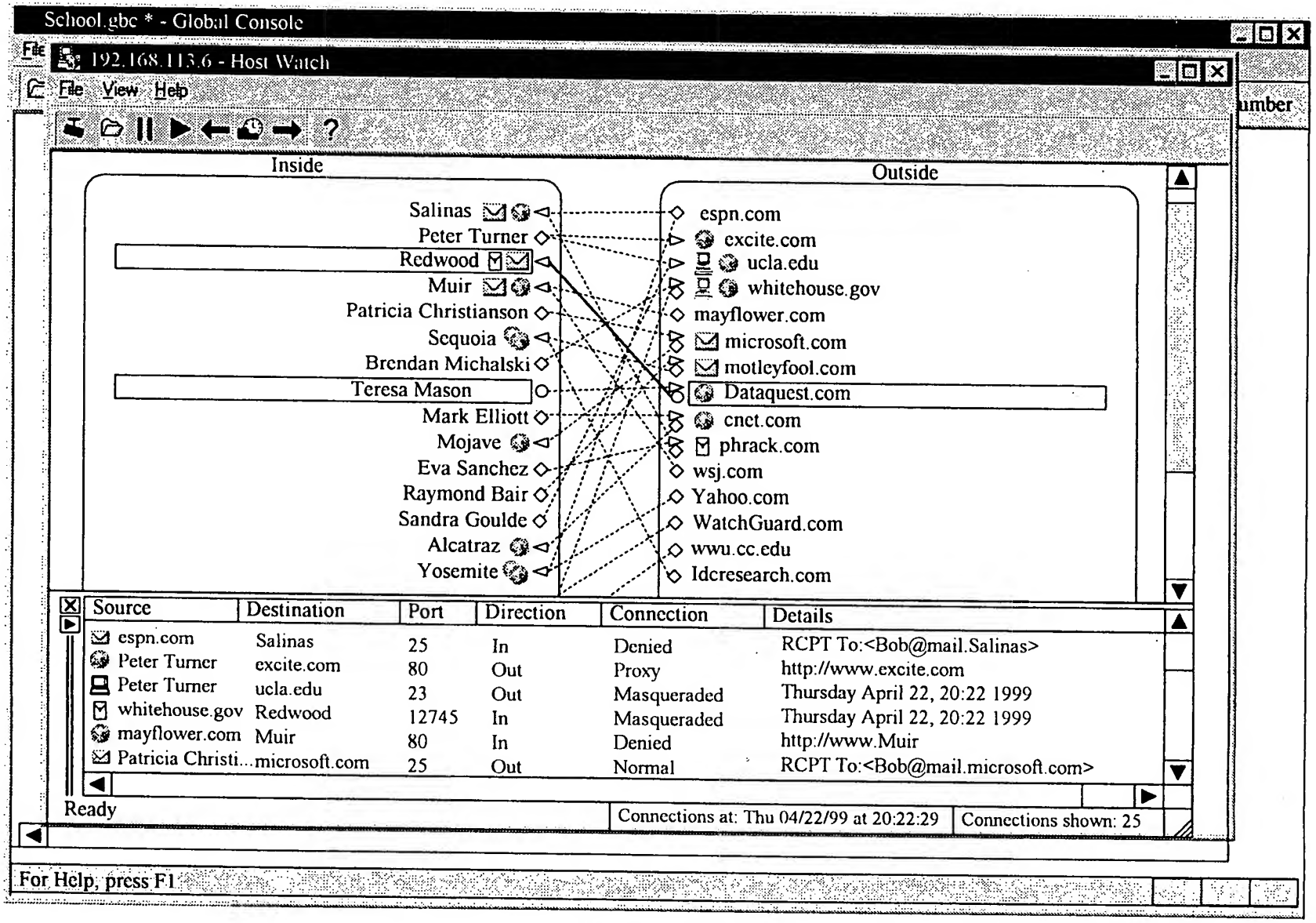
School.gbc * - Global Console
192.168.113.6 - Host Watch
File View Help
Inside
Outside
Salinas
Peter Turner
Redwood
Muir
Patricia Christianson
Sequoia
Brendan Michalski
Teresa Mason
Mark Elliott
Mojave
Eva Sanchez
Raymond Bair
Sandra Goulde
Alcatraz
Yosemite
espn.com
excite.com
ucla.edu
whitehouse.gov
mayflower.com
microsoft.com
motleyfool.com
Dataquest.com
cnet.com
phrack.com
wsj.com
Yahoo.com
WatchGuard.com
wwu.cc.edu
Idcresearch.com
Source | Destination | Port | Direction | Connection | Details
espn.com | Salinas | 25 | In | Denied | RCPT To:<Bob@mail.Salinas>
Peter Turner | excite.com | 80 | Out | Proxy | http://www.excite.com
Peter Turner | ucla.edu | 23 | Out | Masqueraded | Thursday April 22, 20:22 1999
whitehouse.gov | Redwood | 12745 | In | Masqueraded | Thursday April 22, 20:22 1999
mayflower.com | Muir | 80 | In | Denied | http://www.Muir
Patricia Christi... | microsoft.com | 25 | Out | Normal | RCPT To:<Bob@mail.microsoft.com>
Ready
Connections at: Thu 04/22/99 at 20:22:29
Connections shown: 25
For Help, press F1

FIG. 5B

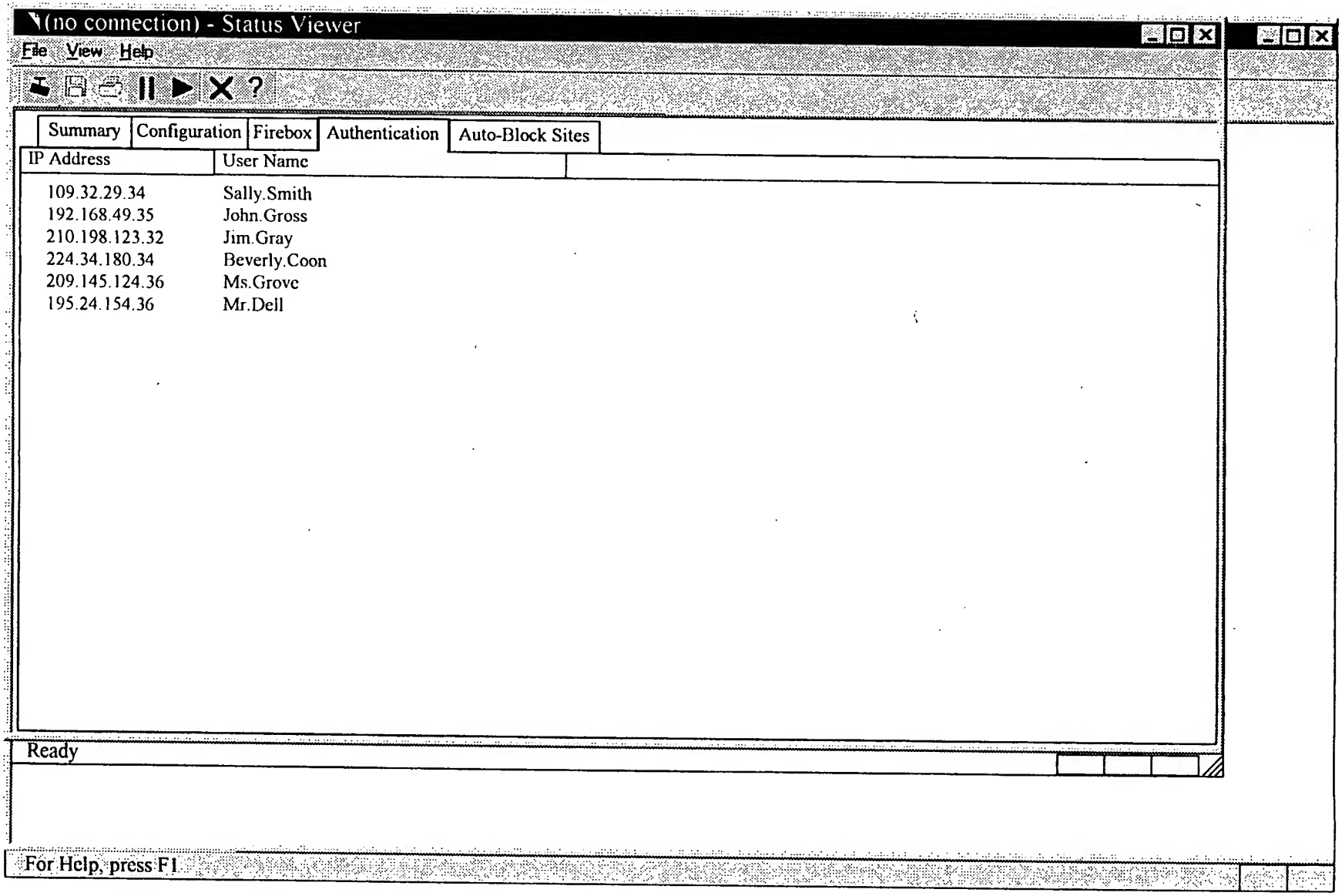
(no connection) - Status Viewer
File View Help
Summary
Configuration
Firebox
Authentication
Auto-Block Sites
IP Address
User Name
109.32.29.34
Sally.Smith
192.168.49.35
John.Gross
210.198.123.32
Jim.Gray
224.34.180.34
Beverly.Coon
209.145.124.36
Ms.Grove
195.24.154.36
Mr.Dell
Ready
For Help, press F1

FIG. 5C

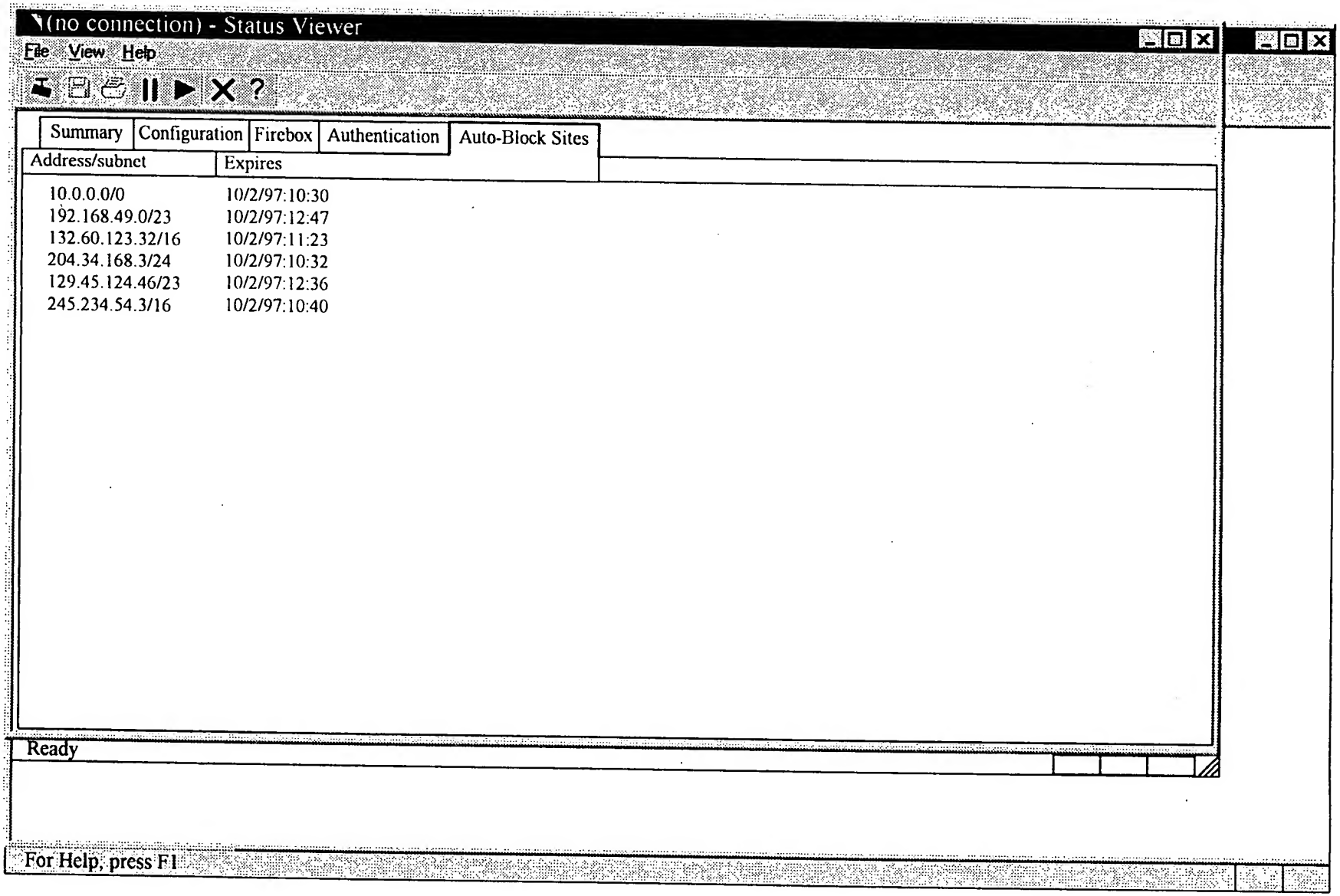
(no connection) - Status Viewer
File View Help
Summary
Configuration
Firebox
Authentication
Auto-Block Sites
Address/subnet
Expires
10.0.0.0/0 10/2/97:10:30
192.168.49.0/23 10/2/97:12:47
132.60.123.32/16 10/2/97:11:23
204.34.168.3/24 10/2/97:10:32
129.45.124.46/23 10/2/97:12:36
245.234.54.3/16 10/2/97:10:40
Ready
For Help, press F1

FIG. 5D

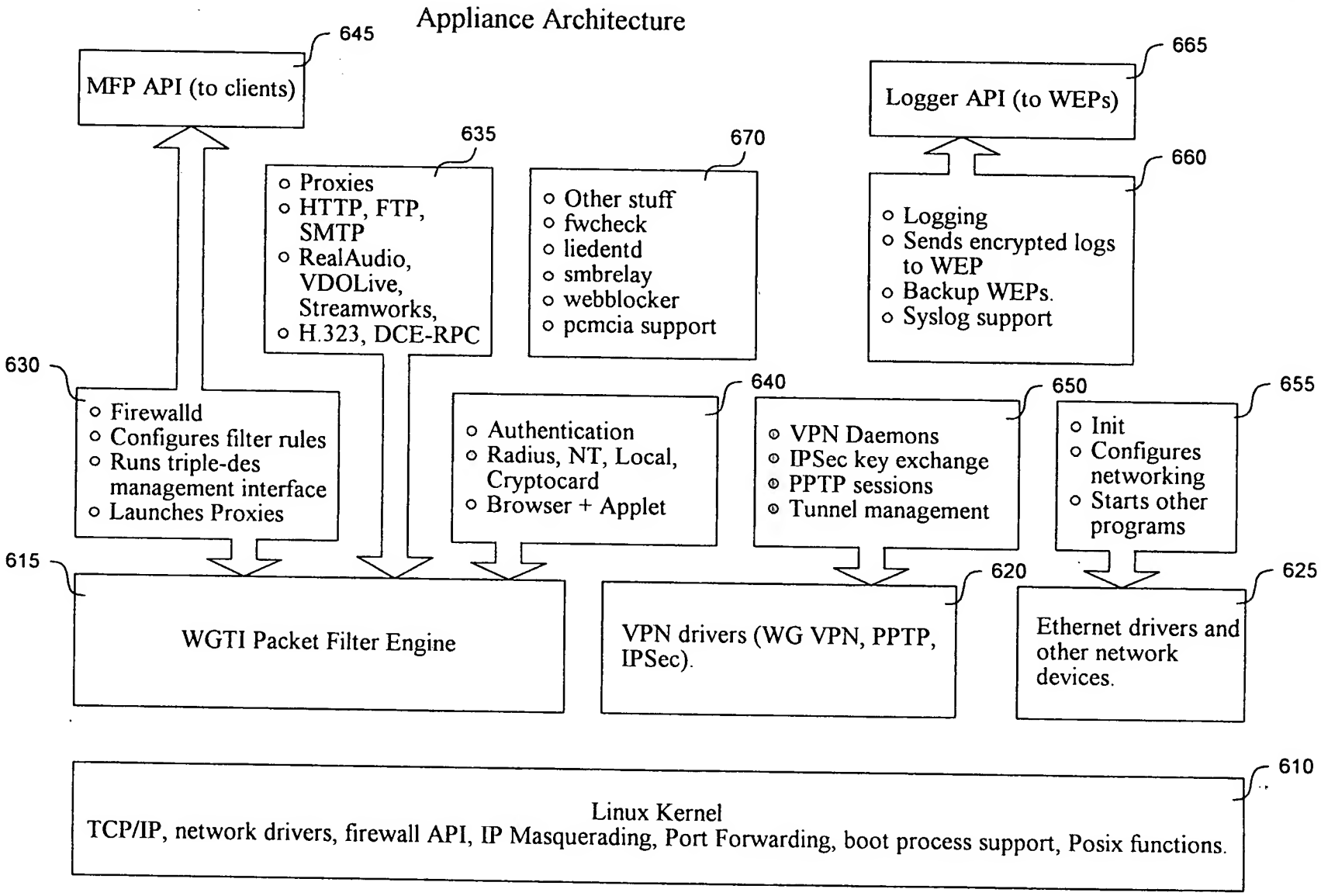
Appliance Architecture
645
MFP API (to clients)
665
Logger API (to WEPs)
635
Proxies
HTTP, FTP, SMTP
RealAudio, VDOLive, Streamworks,
H.323, DCE-RPC
670
Other stuff
fwcheck
liedentd
smbrelay
webblocker
pcmcia support
660
Logging
Sends encrypted logs to WEP
Backup WEPs.
Syslog support
630
Firewalld
Configures filter rules
Runs triple-des management interface
Launches Proxies
640
Authentication
Radius, NT, Local, Cryptocard
Browser + Applet
650
VPN Daemons
IPSec key exchange
PPTP sessions
Tunnel management
655
Init
Configures networking
Starts other programs
615
WGTI Packet Filter Engine
620
VPN drivers (WG VPN, PPTP, IPSec).
625
Ethernet drivers and other network devices.
610
Linux Kernel
TCP/IP, network drivers, firewall API, IP Masquerading, Port Forwarding, boot process support, Posix functions.

FIG. 6

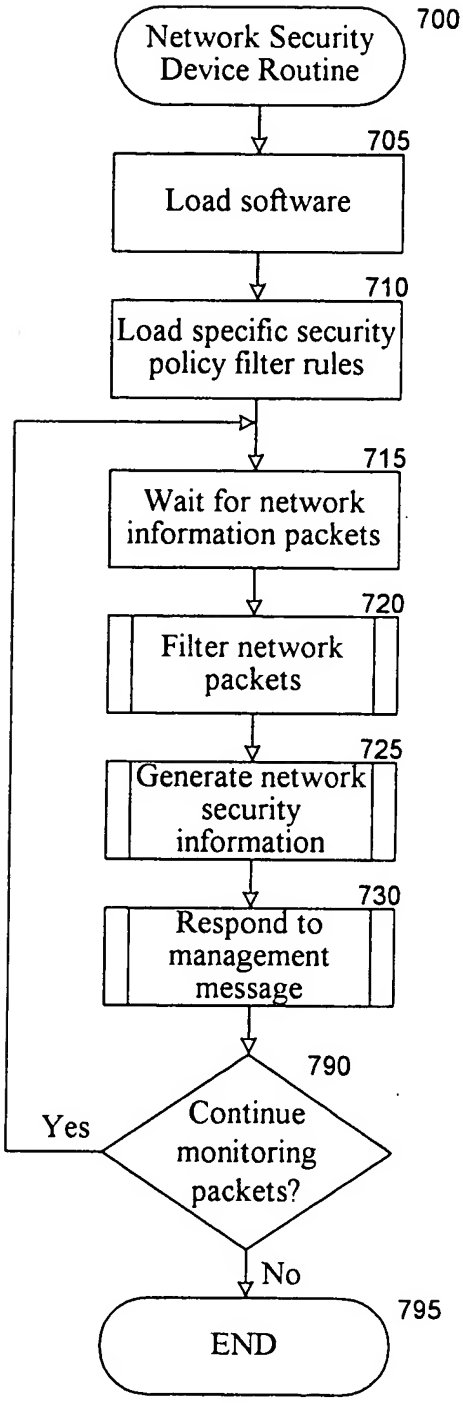
Network Security Device Routine
700
Load software
705
Load specific security policy filter rules
710
Wait for network information packets
715
Filter network packets
720
Generate network security information
725
Respond to management message
730
Continue monitoring packets?
790
Yes
No
END
795

Fig. 7

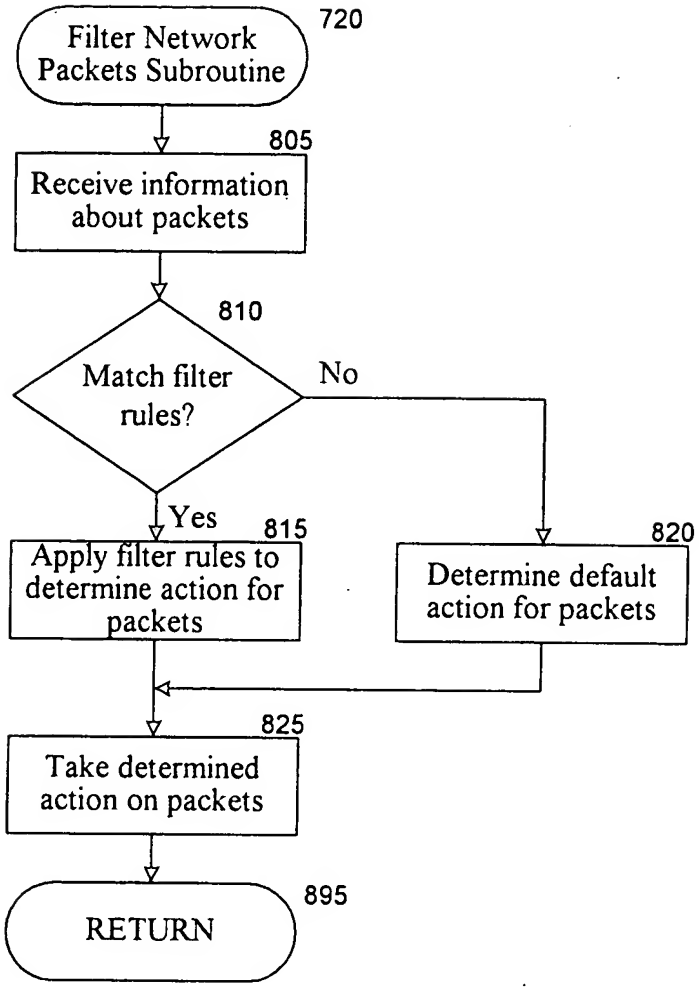
Filter Network Packets Subroutine
720
805
Receive information about packets
810
Match filter rules?
No
Yes
815
Apply filter rules to determine action for packets
820
Determine default action for packets
825
Take determined action on packets
895
RETURN

Fig. 8

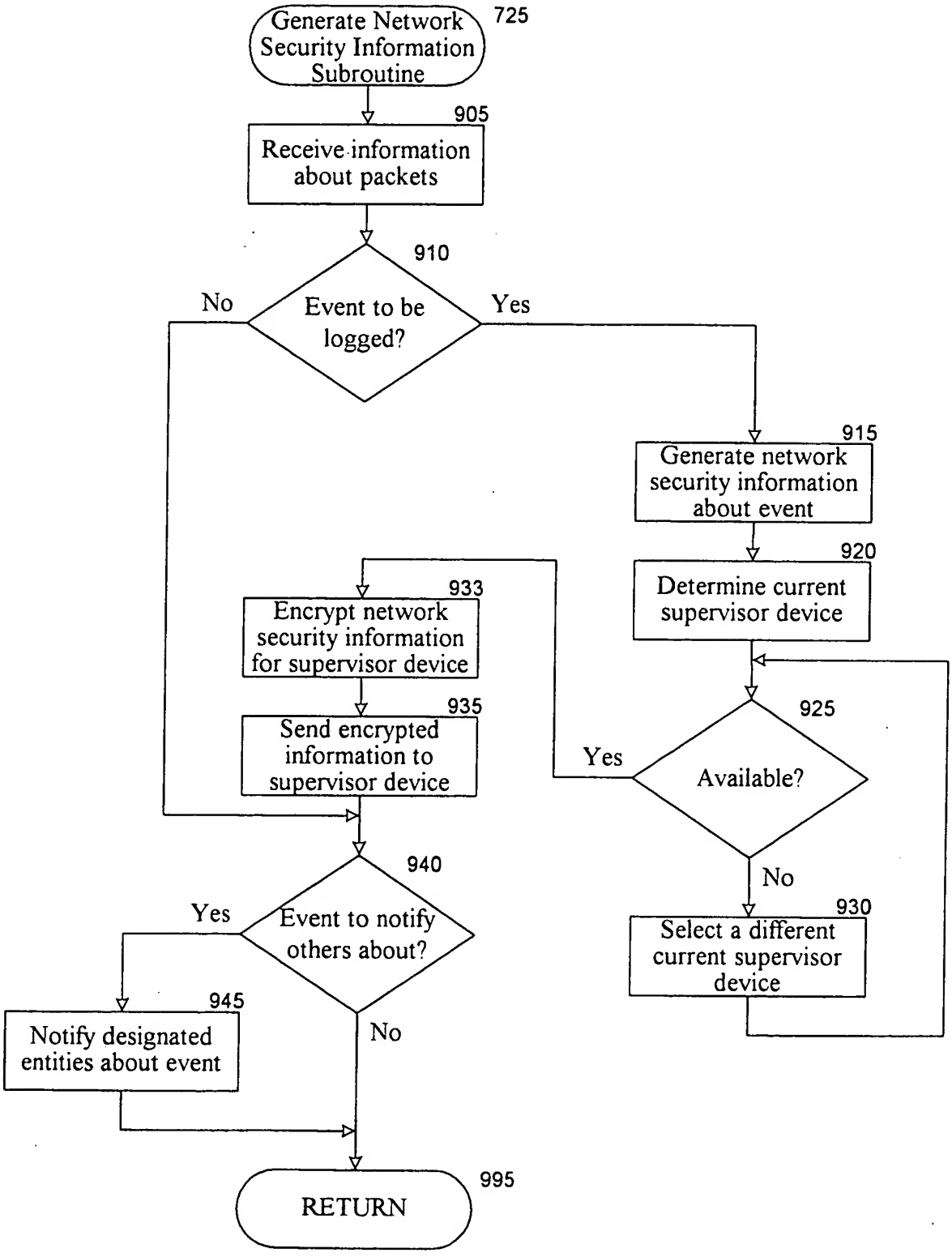
Generate Network Security Information Subroutine
725
905
Receive information about packets
910
Event to be logged?
No
Yes
915
Generate network security information about event
920
Determine current supervisor device
933
Encrypt network security information for supervisor device
935
Send encrypted information to supervisor device
925
Available?
Yes
No
930
Select a different current supervisor device
940
Event to notify others about?
Yes
No
945
Notify designated entities about event
995
RETURN

Fig. 9

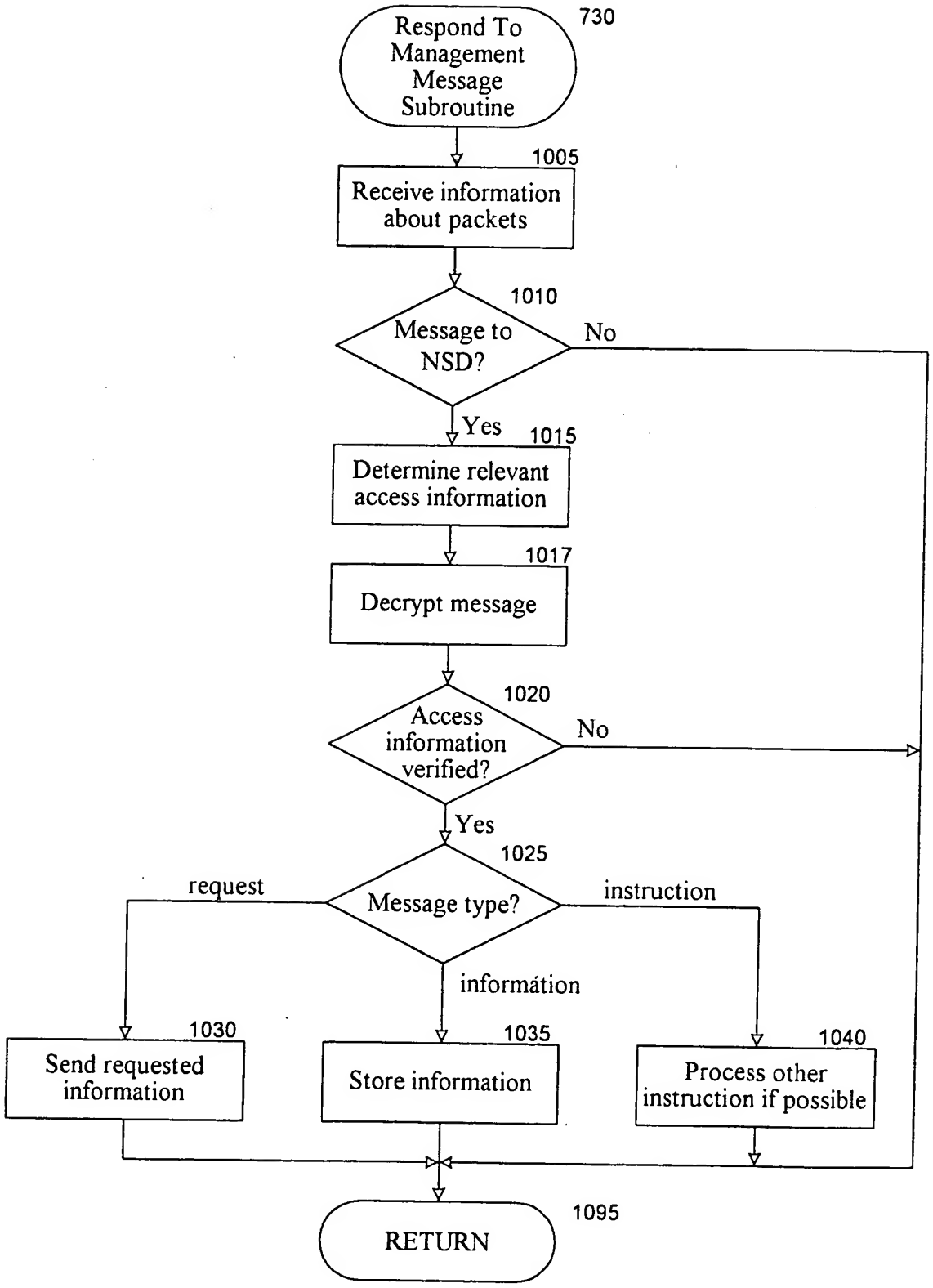
Respond To Management Message Subroutine
730
1005
Receive information about packets
1010
Message to NSD?
No
Yes
1015
Determine relevant access information
1017
Decrypt message
1020
Access information verified?
No
Yes
1025
Message type?
request
instruction
information
1030
Send requested information
1035
Store information
1040
Process other instruction if possible
1095
RETURN

Fig. 10

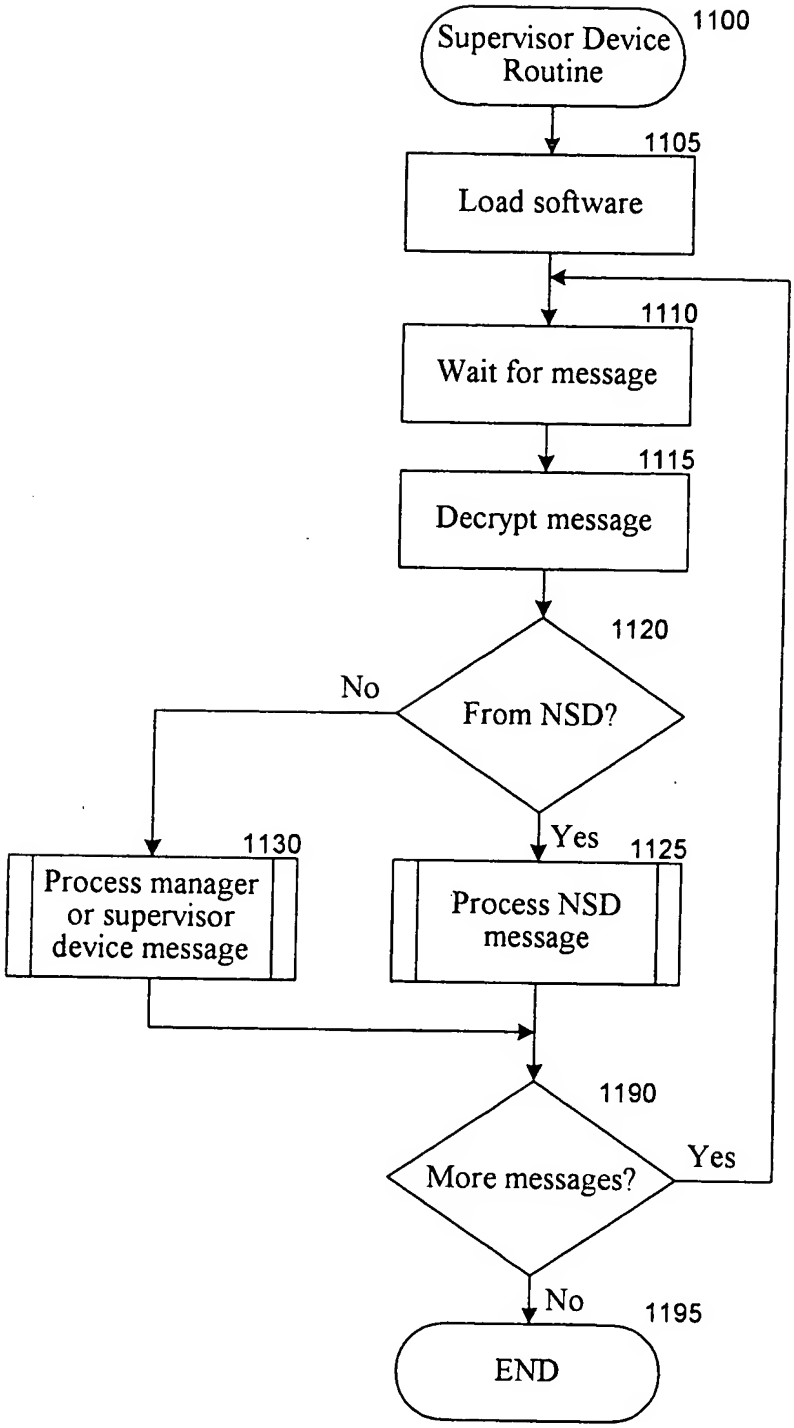
Supervisor Device Routine
1100
1105
Load software
1110
Wait for message
1115
Decrypt message
1120
From NSD?
No
Yes
1130
Process manager or supervisor device message
1125
Process NSD message
1190
More messages?
Yes
No
1195
END

Fig. 11

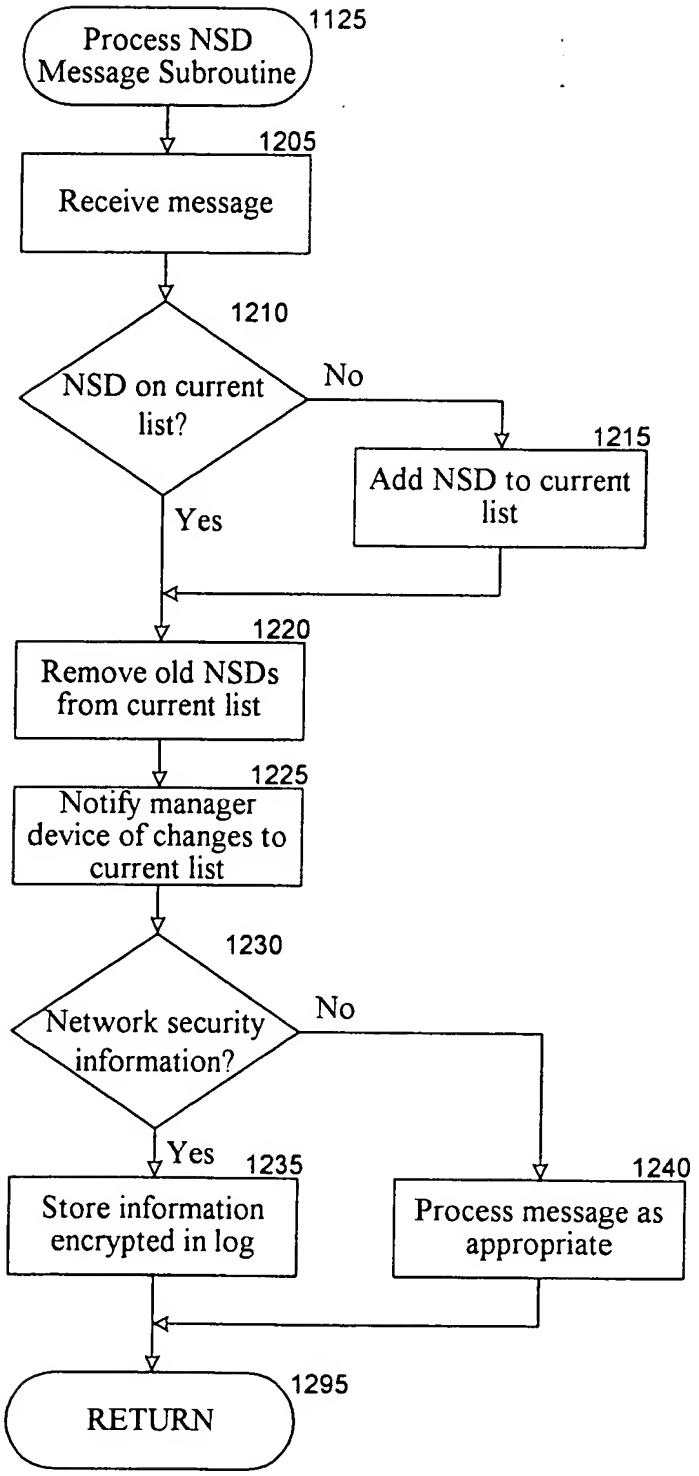
Process NSD Message Subroutine
1125
1205
Receive message
1210
NSD on current list?
No
1215
Add NSD to current list
Yes
1220
Remove old NSDs from current list
1225
Notify manager device of changes to current list
1230
Network security information?
No
Yes
1235
Store information encrypted in log
1240
Process message as appropriate
1295
RETURN

Fig. 12

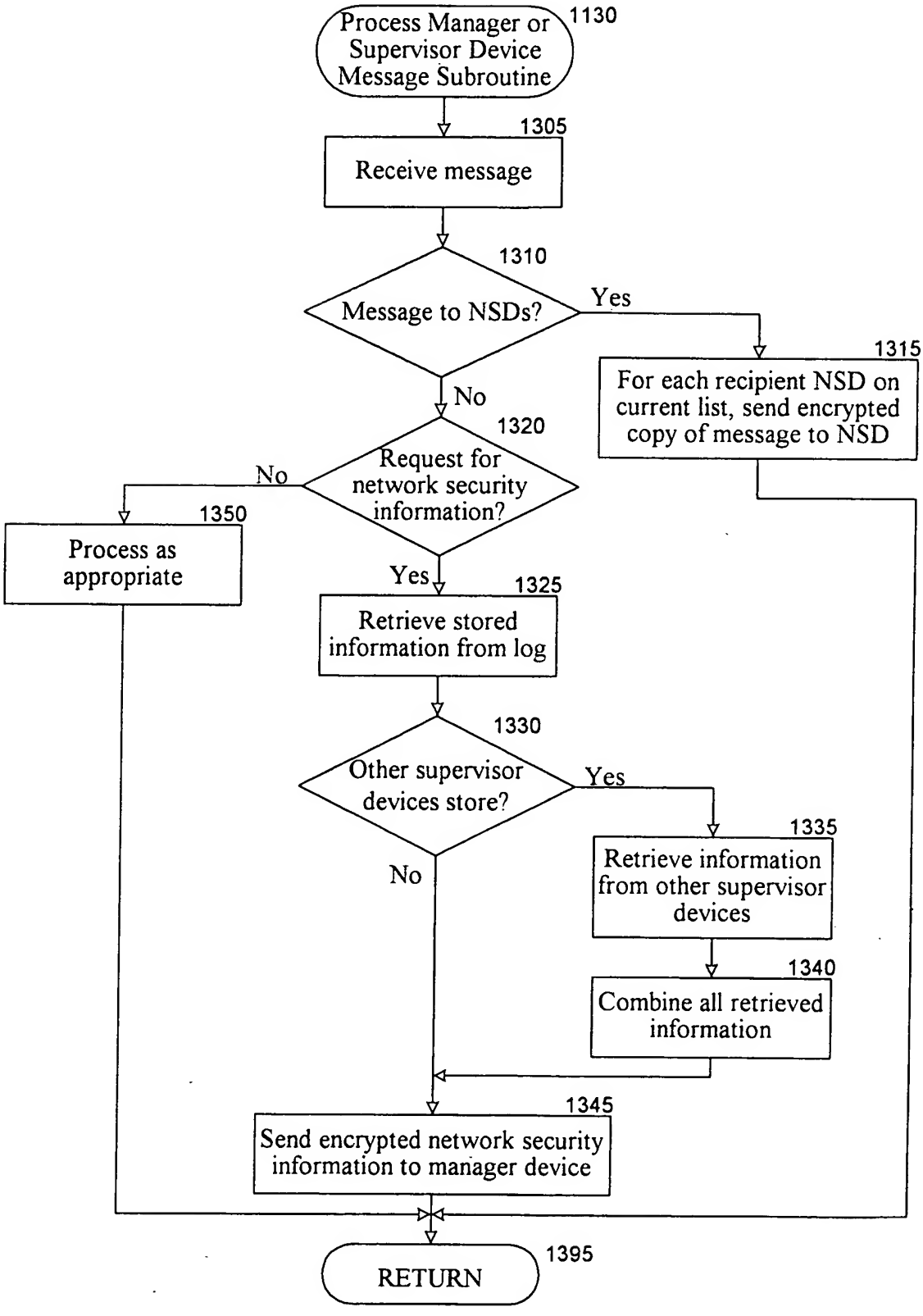
Process Manager or Supervisor Device Message Subroutine
1130
1305
Receive message
1310
Message to NSDs?
Yes
1315
For each recipient NSD on current list, send encrypted copy of message to NSD
No
1320
Request for network security information?
No
1350
Process as appropriate
Yes
1325
Retrieve stored information from log
1330
Other supervisor devices store?
Yes
1335
Retrieve information from other supervisor devices
No
1340
Combine all retrieved information
1345
Send encrypted network security information to manager device
RETURN
1395

Fig. 13

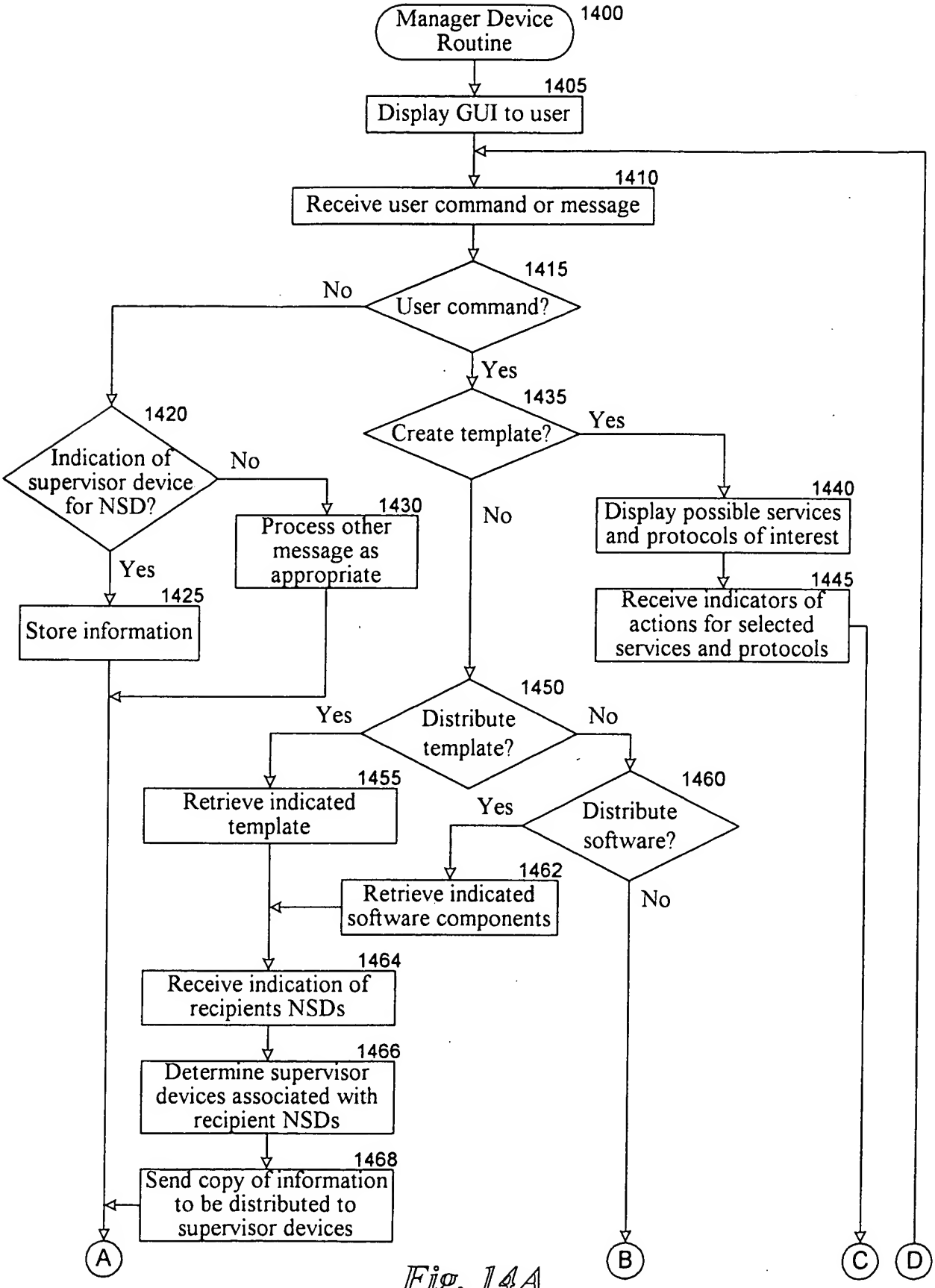
Manager Device Routine
1400
1405
Display GUI to user
1410
Receive user command or message
1415
User command?
No
Yes
1420
Indication of supervisor device for NSD?
No
Yes
1425
Store information
1430
Process other message as appropriate
1435
Create template?
Yes
No
1440
Display possible services and protocols of interest
1445
Receive indicators of actions for selected services and protocols
1450
Distribute template?
Yes
No
1455
Retrieve indicated template
1460
Distribute software?
Yes
No
1462
Retrieve indicated software components
1464
Receive indication of recipients NSDs
1466
Determine supervisor devices associated with recipient NSDs
1468
Send copy of information to be distributed to supervisor devices
A
B
C
D

Fig. 14A

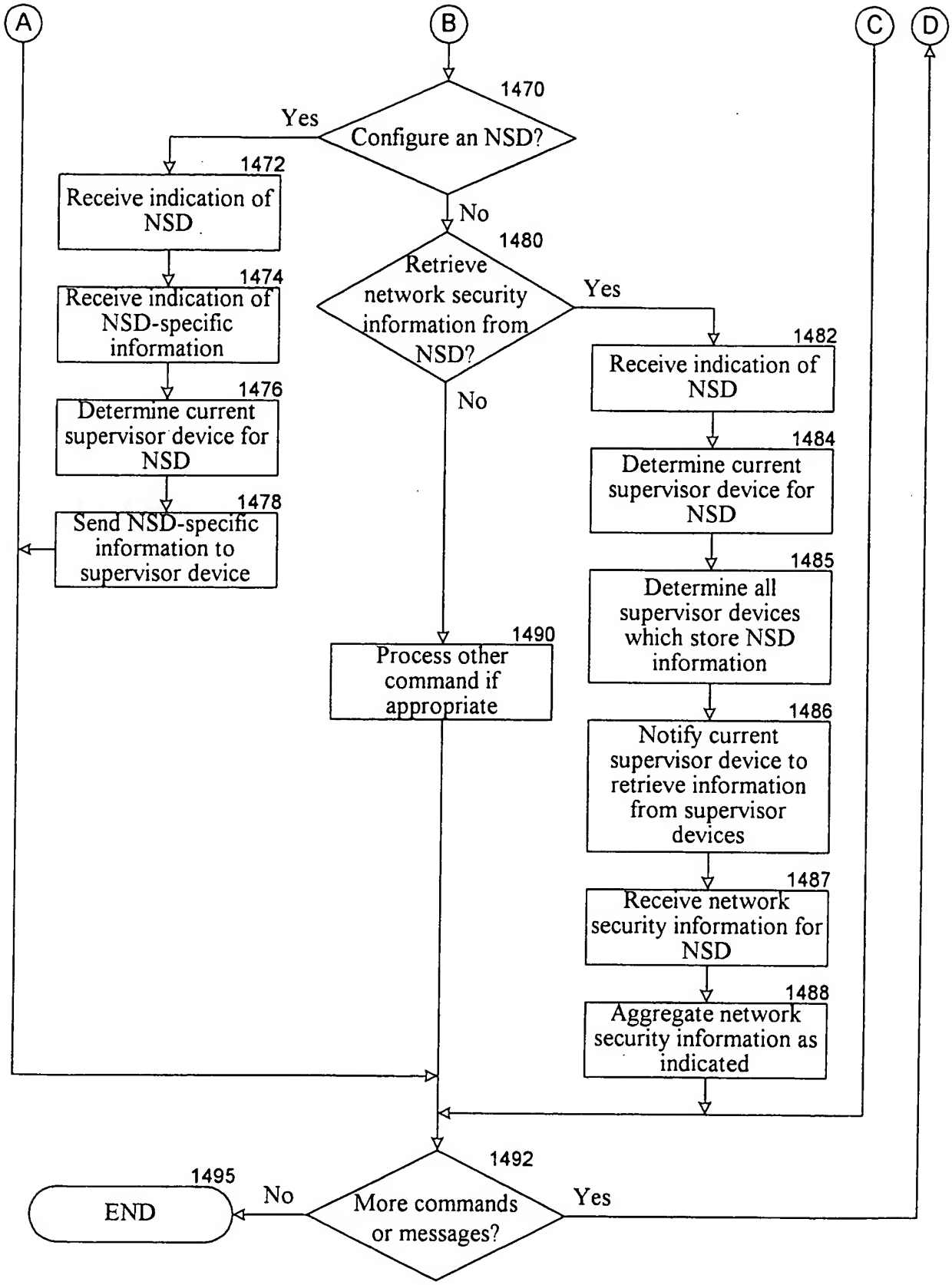
A
B
C
D
1470
Configure an NSD?
Yes
No
1472
Receive indication of NSD
1474
Receive indication of NSD-specific information
1476
Determine current supervisor device for NSD
1478
Send NSD-specific information to supervisor device
1480
Retrieve network security information from NSD?
Yes
No
1482
Receive indication of NSD
1484
Determine current supervisor device for NSD
1485
Determine all supervisor devices which store NSD information
1486
Notify current supervisor device to retrieve information from supervisor devices
1487
Receive network security information for NSD
1488
Aggregate network security information as indicated
1490
Process other command if appropriate
1492
More commands or messages?
No
Yes
1495
END

Fig. 14B